

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-49867

(P2000-49867A)

(43) 公開日 平成12年2月18日 (2000.2.18)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 A
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C
12/28			

審査請求 未請求 請求項の数18 O L (全 16 頁)

(21) 出願番号 特願平11-151071

(22) 出願日 平成11年5月31日 (1999.5.31)

(31) 優先権主張番号 09/087823

(32) 優先日 平成10年5月29日 (1998.5.29)

(33) 優先権主張国 米国 (US)

(71) 出願人 591064003

サン・マイクロシステムズ・インコーポレ
ーテッドSUN MICROSYSTEMS, IN
CORPORATEDアメリカ合衆国 94303 カリフォルニア
州・パロ アルト・サン アントニオ ロ
ード・901

(74) 代理人 100064621

弁理士 山川 政樹

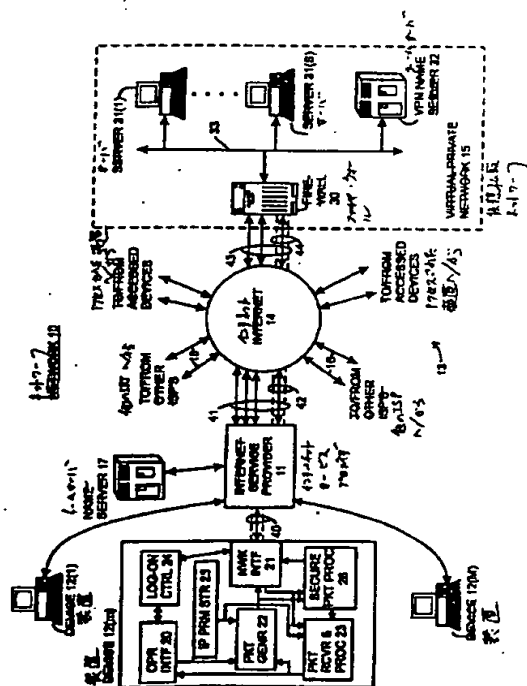
最終頁に続く

(54) 【発明の名称】 インターネットなどの公衆ネットワークに接続された装置とネットワークに接続された装置との通信を容易にするシステムおよび方法

(57) 【要約】

【課題】 仮想私設ネットワーク内の内部装置と外部装置との通信時のインターネットの人間可読アドレスなどの二次アドレスからネットワーク・アドレスへの変換を容易にするシステム。

【解決手段】 仮想私設ネットワークはファイアウォールと、少なくとも1つの内部装置と、ネームサーバとを有する。それぞれネットワーク・アドレスを有する。内部装置は二次アドレスも有し、ネームサーバは二次アドレスとネットワーク・アドレスとの間を関連づける。ファイアウォールは、外部装置との接続の確立を求める外部装置からの要求に応答し、外部装置にネームサーバのネットワーク・アドレスを供給する。外部装置は、内部装置の二次アドレスを含む、内部装置へのアクセスを要求する操作者などからの要求に応答してネットワーク・アドレス要求メッセージを生成し、ファイアウォールとの接続を介して送信し、二次アドレスに関連づけられたネットワーク・アドレスの変換を要求する。



【特許請求の範囲】

【請求項1】 デジタル・ネットワークを介して通信する仮想私設ネットワークと外部装置とを含むシステムであって、

前記仮想私設ネットワークは、それぞれネットワーク・アドレスを有するファイアウォールと、少なくとも1つの内部装置と、ネームサーバとを有し、前記内部装置は二次アドレスも有し、前記ネームサーバは前記二次アドレスと前記ネットワーク・アドレスとの間を関連づけるように構成され、

前記ファイアウォールは、そのファイアウォールと外部装置との間の接続の確立を求める外部装置からの要求に回答し、その外部装置に前記ネームサーバのネットワーク・アドレスを供給するように構成され、

前記外部装置は、前記内部装置の二次アドレスを含む前記内部装置へのアクセスを要求する要求に回答し、前記ファイアウォールへの接続を介して送信するために、前記二次アドレスに関連づけられた前記ネットワーク・アドレスの変換を要求するネットワーク・アドレス要求メッセージを生成し、前記ファイアウォールは前記ネームサーバに前記アドレス変換要求を供給するように構成され、前記ネームサーバは前記二次アドレスに関連づけられた前記ネットワーク・アドレスを供給するように構成され、前記ファイアウォールはさらに前記外部装置への接続を介して送信するためにネットワーク・アドレス応答メッセージで前記ネットワーク・アドレスを供給するように構成されたシステム。

【請求項2】 前記外部装置が、前記内部装置への送信のために少なくとも1つのメッセージを生成する際に前記ネットワーク・アドレス応答メッセージで供給された前記ネットワーク・アドレスを使用するように構成された請求項1に記載のシステム。

【請求項3】 前記外部装置がネットワーク・サービス・プロバイダを介して前記ネットワークに接続された請求項1に記載のシステム。

【請求項4】 前記外部装置が、前記ネットワーク・サービス・プロバイダとの通信セッションを確立するように構成され、前記ネットワーク・サービス・プロバイダが前記外部装置に他のネームサーバの識別情報を提供し、前記他のネームサーバは少なくとも1つの装置のために二次アドレスとネットワーク・アドレスとの間を関連づけるように構成された請求項3に記載のシステム。

【請求項5】 前記外部装置が、前記外部装置に知らされているネームサーバのリストを維持するように構成され、前記外部装置が他の装置へのアクセスを要求する要求に回答して、前記外部装置がネットワーク・アドレスを受け取るまで前記リスト内のネームサーバのうちの連続したネームサーバに問い合わせるように構成され、前記要求が前記他の装置の二次アドレスを含み、各問い合わせで前記外部装置がネットワークを介して送信するた

めに、前記リスト内の前記ネームサーバのうちの1つのネームサーバによる応答を求める前記ネットワーク・アドレス要求メッセージを生成し、前記1つのネームサーバからネットワーク・アドレス応答メッセージを受け取るように構成された請求項1に記載のシステム。

【請求項6】 前記外部装置と前記ファイアウォールとの間の接続が、前記外部装置と前記ファイアウォールとの間で伝送されるメッセージの少なくとも一部が暗号化されるセキュア・トンネルである請求項1に記載のシステム。

【請求項7】 仮想私設ネットワークが、それぞれネットワーク・アドレスを有するファイアウォールと少なくとも1つの内部装置とネームサーバとを有し、前記内部装置は二次アドレスも有し、前記ネームサーバが前記二次アドレスと前記ネットワーク・アドレスとの間を関連づけるように構成された、デジタル・ネットワークによって相互接続された仮想私設ネットワークと外部装置とを含むシステムを動作させる方法であって、

A. 前記ファイアウォールと外部装置との間の接続の確立を求める外部装置からの要求に回答してファイアウォールをイネーブルし、その外部装置に前記ネームサーバのネットワーク・アドレスを供給するステップと、

B. (i) 前記外部装置が、前記内部装置の二次アドレスを含む前記内部装置へのアクセスを要求する要求に回答して、前記ファイアウォールへの接続を介して送信するために、前記二次アドレスに関連づけられた前記ネットワーク・アドレスの変換を要求するネットワーク・アドレス要求メッセージを生成するステップと、

(ii) 前記ファイアウォールが、前記ネームサーバに前記アドレス変換要求を供給するステップと、

(iii) 前記ネームサーバが、前記二次アドレスに関連づけられた前記ネットワーク・アドレスを供給するステップと、

(iv) 前記ファイアウォールが、前記外部装置への接続を介して送信するためにネットワーク・アドレス応答メッセージで前記ネットワーク・アドレスを供給するステップとを含む方法。

【請求項8】 前記外部装置がさらに、前記内部装置への送信のために少なくとも1つのメッセージを生成する際に前記ネットワーク・アドレス応答メッセージで供給された前記ネットワーク・アドレスを使用することができるようになる請求項7に記載のシステム。

【請求項9】 前記外部装置がネットワーク・サービス・プロバイダを介して前記ネットワークに接続できるようにされる請求項7に記載のシステム。

【請求項10】 前記外部装置が、前記ネットワーク・サービス・プロバイダとの通信セッションを確立することができるようになる、前記ネットワーク・サービス・プロバイダが前記外部装置に他のネームサーバの識別情報を提供することができるようになる、前記他のネーム

サーバは少なくとも1つの装置のために二次アドレスとネットワーク・アドレスとの間の関連づけを提供することができるようにされる請求項9に記載のシステム。

【請求項11】 前記外部装置が、前記外部装置に知られているネームサーバのリストを維持することができるようにされ、前記外部装置が他の装置へのアクセスを要求する要求に応答して、前記外部装置がネットワーク・アドレスを受け取るまで前記リスト内のネームサーバのうちの連続したネームサーバに問い合わせることができるようにされ、前記要求が前記他の装置の二次アドレスを含み、各問い合わせで前記外部装置がネットワークを介して送信するために、前記リスト内の前記ネームサーバのうちの1つのネームサーバによる応答を求める前記ネットワーク・アドレス要求メッセージを生成し、前記1つのネームサーバからネットワーク・アドレス応答メッセージを受け取ることができるようにされる請求項7に記載のシステム。

【請求項12】 前記外部装置と前記ファイアウォールとの間の接続が、前記外部装置と前記ファイアウォールとの間で伝送されるメッセージの少なくとも一部が暗号化されるセキュア・トンネルである請求項7に記載の方法。

【請求項13】 仮想私設ネットワークが、それぞれネットワーク・アドレスを有するファイアウォールと、少なくとも1つの内部装置と、ネームサーバとを有し、前記内部装置は二次アドレスも有し、前記ネームサーバは前記二次アドレスと前記ネットワーク・アドレスとの間を関連づけるように構成された、デジタル・ネットワークによって相互接続された仮想私設ネットワークと外部装置との接続に使用するコンピュータ・プログラム製品であって、

A. 前記ファイアウォールが、そのファイアウォールと外部装置との間の接続の確立を求める外部装置からの要求に応答し、前記外部装置に前記ネームサーバのネットワーク・アドレスを供給することができるようにするよう構成されたネームサーバ識別コード・モジュールと、

B. 前記外部装置が、前記内部装置の二次アドレスを含む前記内部装置へのアクセスを要求する要求に応答し、前記ファイアウォールへの接続を介して送信するために、前記二次アドレスに関連づけられた前記ネットワーク・アドレスの変換を要求するネットワーク・アドレス要求メッセージを生成することができるようにするネットワーク・アドレス要求メッセージ生成コード・モジュールと、

C. 前記ファイアウォールが、前記ネームサーバに前記アドレス変換要求を供給することができるようにするアドレス変換要求転送モジュールと、

D. 前記ネームサーバが前記二次アドレスに関連づけられた前記ネットワーク・アドレスを供給することができ

るようにするネームサーバ制御モジュールと、

E. 前記ファイアウォールが、前記外部装置への接続を介して送信するためにネットワーク・アドレス応答メッセージで前記ネットワーク・アドレスを供給することができるようにするネットワーク・アドレス応答メッセージ転送モジュールとがコード化された機械可読媒体を含むコンピュータ・プログラム製品。

【請求項14】 前記外部装置が前記内部装置への送信のために少なくとも1つのメッセージを生成する際に前記ネットワーク・アドレス応答メッセージで供給された前記ネットワーク・アドレスを使用することができるようにするよう構成されたネットワーク・アドレス使用モジュールをさらに含む請求項13に記載のコンピュータ・プログラム製品。

【請求項15】 前記外部装置がネットワーク・サービス・プロバイダを介して前記ネットワークに接続できるようにするネットワーク・サービス・プロバイダ制御モジュールをさらに含む請求項13に記載のコンピュータ・プログラム製品。

【請求項16】 前記ネットワーク・サービス・プロバイダ制御モジュールが、前記外部装置を前記ネットワーク・サービス・プロバイダとの通信セッションのためにイネーブルにし、前記ネットワーク・サービス・プロバイダから他のネームサーバの識別情報を受け取ることができるようにする、通信セッション確立モジュールを含む請求項15に記載のコンピュータ・プログラム製品。

【請求項17】 前記外部装置が前記外部装置に知られているネームサーバのリストを維持することができる、前記外部装置が他の装置へのアクセスを要求する要求に応答して、前記外部装置がネットワーク・アドレスを受け取るまで前記リスト内のネームサーバのうちの連続したネームサーバに問い合わせることができるようにするネームサーバ問い合わせ制御モジュールであって、前記要求が前記他の装置の二次アドレスを含み、各問い合わせで前記外部装置がネットワークを介して送信するために、前記リスト内の前記ネームサーバのうちの1つのネームサーバによる応答を求める前記ネットワーク・アドレス要求メッセージを生成し、前記1つのネームサーバからネットワーク・アドレス応答メッセージを受け取ることができるようにするネームサーバ問い合わせ制御モジュールをさらに含む請求項13に記載のコンピュータ・プログラム製品。

【請求項18】 前記外部装置と前記ファイアウォールとの間の接続が、前記外部装置と前記ファイアウォールとの間で伝送されるメッセージの少なくとも一部が暗号化されるセキュア・トンネルである請求項14に記載のコンピュータ・プログラム製品。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般にはディジタ

ル通信システムおよび方法に関し、より詳細には、インターネットなどの公衆ネットワークに接続された装置と私設ネットワークに接続された装置との間の通信を容易にするシステムおよび方法に関する。

【0002】

【従来の技術】 デジタル・コンピュータ・システムおよびその他のデジタル装置間でのデータおよびプログラムを含む情報の伝送を容易にするために、デジタル・ネットワークが開発されている。多様な情報伝送方法を使用して情報を伝送する、いわゆる「ワイド・エリア・ネットワーク」(WAN)や「ローカル・エリア・ネットワーク」(LAN)を含む様々なタイプのネットワークが開発され、実施されている。一般に、LANは、特定の事務所、会社、またはより小規模なタイプの組織内で特定の情報を伝送するために、個々の事務所施設内などの比較的狭い地理的区域にわたって実施される。他方、WANは一般に、比較的広い地理的区域にわたって実施され、LAN間およびLANに接続されていない装置間で情報を伝送するために使用することができる。WANは、複数の会社のために情報を伝達することができるインターネットなどの公衆ネットワークも含む。

【0003】 ネットワーク、特に、インターネットなどの大規模な公衆WANを介した通信に関してはいくつかの問題が生じている。一般に、情報はメッセージ・パケットの形でネットワークを介して伝送され、パケットは送信元装置としての1つの装置から宛先装置としての他の装置に、ネットワーク内の1つまたは複数のルータまたはスイッチング・ノード(一般にはスイッチング・ノード)を介して伝送される。各メッセージ・パケットは宛先アドレスを含み、スイッチング・ノードはそれを使用してそれぞれのメッセージ・パケットを適切な宛先装置に経路指定する。インターネットを介したアドレスは、「n」ビット整数の形式(「n」は32または128)であり、人が覚えたり、メッセージ・パケットを送信できるようにしたい場合にそれを入力したりするのが難しい。ユーザが特定の整数インターネットアドレスを覚えたり入力したりする必要を軽減するために、インターネットは、それぞれの装置の操作者によってより容易に使用される第2のアドレス指定機構を備える。このアドレス指定機構では、インターネットに接続されたLAN、インターネット・サービス・プロバイダ(「ISP」)などのインターネット・ドメインが、比較的人間が読みやすい名前で識別される。この人間可読名の使用に対応するために、DNSサーバとも呼ばれるネームサーバが設けられ、人間可読名を適切なインターネット・アドレスに変換する。1台の装置の操作者が、メッセージ・パケットを他の装置に送信しようとして他方の装置の人間可読名を入力すると、その装置は最初にネームサーバに接触する。一般に、ネームサーバはISP自体の一部とするか、またはISPを介してインターネットで

アクセス可能な特定の装置とすることができる。いずれの場合も、ISPは、装置がISPにログインすると、使用するネームサーバをその装置に知らせる。装置によって接触された後で、ネームサーバがその人間可読ドメイン名の整数インターネット・アドレスを持っているかまたは入手可能な場合、ネームサーバはその人間可読ドメイン名に対応する整数インターネット・アドレスを操作者の装置に提供する。その後、装置はネームサーバによって返された整数インターネット・アドレスをメッセージ・パケットに入れ、そのメッセージ・パケットを従来の方式でインターネットを介して送信するためにISPに供給する。インターネット・スイッチング・ノードは、整数インターネット・アドレスを使用してメッセージ・パケットを意図された宛先装置に経路指定する。

【0004】 特にインターネットなどの公衆WANを介した情報伝送に関しては他の問題も生じる。1つの問題は、WANを介して転送される情報であって、送信元装置と宛先装置が機密にしておきたい情報が、その情報を傍受する可能性のある盗聴者に対して機密に維持されるように保証することである。機密性を維持するには、様々な形態の暗号化が開発され、送信元装置による伝送の前に情報を暗号化し、宛先装置によって受け取られた後で情報を復号するために使用されている。たとえば、特定の送信元装置と特定の宛先装置との間で伝送されるすべての情報を機密に維持することが望ましい場合、それらの装置は両者の間に「セキュア・トンネル」を設定することができる。このセキュア・トンネルは本質的に、伝送の前に送信元装置によって宛先装置に伝送されるすべての情報(ただし、アドレス情報など、送信元装置と宛先装置の間のネットワークを介したネットワーク・パケットの流れを制御する特定のプロトコル情報は除く)が暗号化されるように保証し、暗号化された情報が宛先装置によって使用される前に復号されるように保証する。送信元装置と宛先装置はそれ自体がそれぞれ暗号化と復号を実行するか、または、メッセージ・パケットがインターネットを介して伝送される前に他の装置が暗号化と復号を行うことができる。

【0005】 特に、LAN、WAN、またはそれらの任意の組合せである私設ネットワークがインターネットなどの公衆WANに接続されている会社、政府機関、および民間組織に対して生じる他の問題は、それらの私設ネットワークが、それらの会社がアクセスさせたくない他者から保護されるように保証すること、またはそれぞれの組織がアクセスを制限したい他者によるアクセスを規制または管理することである。これに対応するために、組織は一般に、その私設ネットワークを「ファイアウォール」と呼ばれることがある限定された数のゲートウェイを介してWANに接続し、内部ネットワークと公衆ネットワークとの間のすべてのネットワーク・トラフィックがこのファイアウォールを通るようにする。一般に、

ファイアウォールの「背後」にある私設ネットワーク内のドメインおよび装置のネットワーク・アドレスは、私設ネットワーク内に設けられたネームサーバにはわかっているが、私設ネットワーク外部のネームサーバやその他の装置には入手できず、私設ネットワーク外部の装置と私設ネットワーク内部の装置との間の通信を困難にする。

【0006】

【発明が解決しようとする課題】本発明は、私設ネットワークに接続されたネームサーバまたは同様のものによるインターネットの人間可読アドレスなどの二次アドレスからネットワーク・アドレスへの変換を容易にすることによって、インターネットなどの公衆ネットワークに接続された装置と私設ネットワークに接続された装置との間の通信を容易にする、新規な改良されたシステムおよび方法を提供する。

【0007】

【課題を解決するための手段】要約すると、本発明は、仮想私設ネットワークと、ディジタル・ネットワークによって相互接続された外部装置とを含むシステムを提供する。仮想私設ネットワークは、ファイアウォールと、少なくとも1つの内部装置と、ネームサーバとを有し、それぞれがネットワーク・アドレスを有する。内部装置は、二次アドレスも有し、ネームサーバは二次アドレスとネットワーク・アドレスとの間の関連づけを行うように構成されている。ファイアウォールは、外部装置との間の接続の確立を求める外部装置からの要求にตอบสนองし、外部装置にネームサーバのネットワーク・アドレスを提供する。外部装置は、内部装置へのアクセスを要求する内部装置の二次アドレスを含む操作者などからの要求にตอบสนองし、ネットワーク・アドレス要求メッセージを生成してファイアウォールまでの接続を介して送信し、二次アドレスに関連づけられたネットワーク・アドレスの変換を要求する。ファイアウォールはそのアドレス変換要求をネームサーバに供給し、ネームサーバは二次アドレスに関連づけられたネットワーク・アドレスをファイアウォールに供給する。ファイアウォールは、外部装置までの接続を介して送信するためにネットワーク・アドレス応答メッセージでネットワーク・アドレスを供給する。その後、外部装置は、このようにして供給されたネットワーク・アドレスを、内部装置宛に意図されたファイアウォールとのその後の通信で使用する事ができる。

【0008】

【発明の実施の形態】本発明は、特許請求の範囲で具体的に示されている。本発明の上記およびその他の利点は、添付図面と共に以下の説明を参照すればよりよく理解できよう。

【0009】図1は、本発明により構成されたネットワーク10を示す機能ブロック図である。図1に図示する

ネットワーク10は、インターネット・サービス・プロバイダ（「ISP」）11に接続された1つまたは複数の装置12（1）～12（M）（一般的に参照番号12（m）で識別する）および参照番号13で一般的に識別されたその他の装置間の、インターネット14を介したメッセージ・パケットの伝送を容易にし、それによって装置12（m）と13と間でのメッセージ・パケットでの情報の伝送を容易にするインターネット・サービス・プロバイダ（「ISP」）11を含む。ISP11は、参照番号41で一般的に識別された1つまたは複数の論理接続またはゲートウェイまたは同様のもの（本明細書では総称して「接続」と呼ぶ）を介してインターネット14に接続する。ISP11は、公衆ISPとすることができ、その場合、一般社会の構成員である操作者が制御することができる装置12（m）に接続され、それらの操作者がインターネットへアクセスできるようにする。あるいは、ISP11は私設ISPとすることができ、その場合、それに接続された装置12（m）は一般に、たとえば特定の会社または政府機関の従業員、民間組織のメンバーなどによって操作され、それらの従業員またはメンバーがインターネットへアクセスできるようにする。

【0010】従来、インターネットは、ISP11および装置13を相互接続してそれらの間のメッセージ・パケットの伝送を容易にするスイッチング・ノード（別途図示せず）の網を含む。インターネット14を介して伝送されるメッセージ・パケットは、いわゆるインターネット・プロトコル「IP」によって定義されたものに準拠し、ヘッダ部分とデータ部分とを含み、誤り検出または訂正あるいはその両方の部分を含むことができる。ヘッダ部分には、たとえば、そのメッセージ・パケットを受け取るべき装置を宛先装置として識別する宛先アドレスと、メッセージ・パケットを生成した装置を識別する送信元アドレスを含めて、インターネット14を介してメッセージ・パケットを伝送するために使用される情報が含まれる。各メッセージ・パケットについて、宛先アドレスと送信元アドレスはいずれも、それぞれの宛先装置と送信元装置を固有に識別する整数の形態をとる。宛先装置がインターネット、またはISP11、あるいはインターネット14に接続されたその他の装置に接続されている場合、インターネット14を構成するスイッチング・ノードは、少なくともそれぞれのメッセージ・パケットの宛先アドレスを使用して、それ（すなわちそれぞれのメッセージ・パケット）を宛先装置に経路指定する。インターネット、またはISP11あるいはインターネットに接続された装置は、そのメッセージ・パケットをその適切な宛先に転送する。各メッセージ・パケットのデータ部分には、メッセージ・パケットで伝送するデータと、メッセージ・パケットが送信元装置から宛先装置に正しく伝送されたことを検証する（誤り検出情報

の場合) ためと、メッセージ・パケットが正しく伝送されなかった場合に選択されたタイプの誤りを訂正する

(誤り訂正情報の場合) ために使用することができる誤り検出および／または訂正情報を含む誤り検出および／または訂正部分とが含まれる。

【0011】ISP11に接続される装置12(m)

は、たとえば、パーソナル・コンピュータ、コンピュータ・ワークステーションなどインターネット14を介して他の装置13と通信するいくつかのタイプの装置のいずれをも含むことができる。各装置12(m)は、装置12(m)がポイントツーポイント・リンクを使用してISP11に接続される場合は周知のポイントツーポイント・プロトコル(「PPP」)、装置12(m)がイーサネットなどの分岐ネットワークを介してISP11に接続される場合は従来の分岐ネットワーク・プロトコルなど、従来の任意のプロトコルを使用して、ISP11と通信し、インターネット14で伝送するためにメッセージ・パケットをISP11に送信するか、またはインターネット14を介してISP11が受け取ったメッセージ・パケットをISP11から受け取る。装置12

(m)は一般に、たとえばシステム・ユニット、ビデオ表示装置、およびキーボードやマウスなどのオペレータ入力装置を含む、従来のプログラム記憶式コンピュータ・アーキテクチャにより構成される。システム・ユニットは、一般に、処理装置、メモリ、ディスクやテープ記憶要素などの大容量記憶装置、およびそれぞれの装置をISP11とインタフェースさせるネットワーク・インタフェース装置または電話インタフェース装置を含むその他の要素(別途に図示せず)を含む。処理装置は、オペレーティング・システムの制御下でアプリケーション・プログラムを含むプログラムを処理し、処理されたデータを生成する。ビデオ表示装置は、装置が処理されたデータと処理状況をユーザに対して表示することができるようにし、オペレータ入力装置は、ユーザがデータを入力し、処理を制御することができるようにする。

【0012】装置12(m)のこれらの装置は、適切なプログラミングと共に、協調動作して、装置12(m)に、たとえばオペレータ・インタフェース20、ネットワーク・インタフェース21、メッセージ・パケット・ジェネレータ22、メッセージ・パケット受信および処理機能要素23、ISPログオン・コントロール24、インターネット・パラメータ・ストア25、および本発明に関係するセキュア・メッセージ・パケット処理機能要素26を含む多くの機能要素を備えている。オペレータ・インタフェース20は、装置12(m)での装置12(m)のオペレータ入力装置からの入力情報の受領と、装置12(m)のビデオ表示装置上での操作者に対する出力情報の表示を容易にする。ネットワーク・インタフェース21は、適切なPPPまたはネットワーク・プロトコルを使用して装置12(m)がISP11に接

続し、ISP11にメッセージ・パケットを送信したり、ISP11からメッセージ・パケットを受け取ったりするのを容易にする。ネットワーク・インタフェース21は、公衆電話ネットワークを介したISP11への接続を容易にし、公衆電話システムを介した装置12

(m)のダイヤルアップ・ネットワーク化を可能にすることもできる。別法として、あるいはそれに加えて、ネットワーク・インタフェース21は、たとえばイーサネットなどの従来のLANによるISP11を介した接続も容易にすることができる。ISPログオン・コントロール24は、オペレーティング・インタフェース20によって供給された入力に応答して、または装置12

(m)によって処理されているプログラム(図示せず)からの要求に응答して、ネットワーク・インタフェース21を介して通信し、装置12(m)とISP11との間の通信セッションの初期設定(「ログオン」)を容易にし、その通信セッション中に装置12(m)はメッセージ・パケットの形でインターネット14を介して他の装置、およびISP11に接続された他の装置12

(m')(m'≠m)または他のISPに情報を送信することができる。ログオン動作中、ISPログオン・コントロール24は、インターネット・プロトコル(「IP」)パラメータを受け取り、このパラメータは通信セッション中にメッセージ・パケット生成と共に使用される。

【0013】通信セッション中、メッセージ・パケット・ジェネレータ22は、オペレーティング・インタフェース20を介して操作者によって供給された入力に응答して、または装置12(m)によって処理されているプログラム(図示せず)からの要求に응答して、ネットワーク・インタフェース21を介した送信のためのメッセージ・パケットを生成する。ネットワーク・インタフェース21は、ISP11からもメッセージ・パケットを受け取ってメッセージ・パケット受信および処理機能要素23に送り、それらを処理させ、オペレータ・インタフェース20または装置12(m)によって処理されているその他のプログラム(図示せず)に供給させる。受け取ったメッセージ・パケットに、操作者に対して表示するウェブ・ページなどの情報が含まれている場合、その情報をオペレータ・インタフェース20に供給し、その装置の表示装置上に情報が表示されるようにすることができる。それに加えて、または別法として、情報は装置12(m)によって処理されている他のプログラム(図示せず)に処理のために供給することもできる。

【0014】一般に、オペレーティング・インタフェース20、メッセージ・パケット・ジェネレータ22、メッセージ受信および処理機能要素23、ISPログオン・コントロール24、およびインターネット・パラメータ・ストア25などの要素は、Mosaic、Netscape Navigator、Microsoft I

Internet Explorerなどの従来のインターネット・ブラウザの要素を含むことができる。

【0015】前述のように、本発明に関連して、装置12(m)はセキュア・メッセージ・パケット処理機能要素26も含む。セキュア・メッセージ・パケット処理機能要素26は、装置12(m)と他の装置12(m')

(m' ≠ m)または13との間での後述の「セキュア・トンネル」の確立と使用を容易にする。一般に、セキュア・トンネルでは、装置12(m)と他の特定の装置12(m')(m' ≠ m)または13との間で伝送されるメッセージ・パケットの少なくともデータ部分内の情報が、たとえば送信元装置で、送信の前にデータ部分を暗号化することによって機密に維持される。このようなメッセージ・パケットの他の部分に入っている情報も機密に維持することができる。ただし、インターネットのスイッチング・ノードおよびISPがメッセージ・パケットを受け取るべき装置を識別することができるように、たとえば少なくとも宛先情報を含めて、装置間のそれぞれのメッセージ・パケットの伝送を助けるのに必要な情報は機密にされていない。

【0016】ISP11に加えて、矢印16でそれぞれ示すように他のいくつかのISPもインターネットに接続することができ、したがって、他の装置を有するそれらの他のISPに接続された装置と、ISP11に接続された装置12(n)を含む他の装置とのインターネットを介した通信も可能になる。

【0017】装置12(m)がアクセスし、通信する装置13も、パーソナル・コンピュータ、コンピュータ・ワークステーションなどを含めて任意の数のタイプの装置とすることができ、これには、ネットワークに直接または間接に接続可能なそのような装置や他の多くのタイプの装置を含む、ミニ・コンピュータ、メインフレーム・コンピュータ、大容量記憶システム、計算サーバ、ローカル・エリア・ネットワーク(「LAN」)およびワイド・エリア・ネットワーク(「WAN」)も含まれる。本発明に関しては、このような装置の少なくとも1つの装置は、仮想私設ネットワーク15として識別される少なくとも1つの私設ネットワークを含み、これはLANまたはWANの形態をとることができる。仮想私設ネットワーク15は、装置12(m')(m' ≠ m)

(ISPを介してインターネット14に接続する)または13(インターネット14に直接接続する)のいずれの装置でも含むことができる。本明細書で説明する例示の実施形態では、仮想私設ネットワーク15は装置13を含むものとする。仮想私設ネットワーク15自体は、本明細書でファイアウォール30として示す複数の装置と、複数のサーバ31(1)～31(S)(一般的に参照番号31(s)で識別する)と、ネームサーバ32とを含み、これらはすべて通信リンク33によって相互接続されている。ファイアウォール30およびサーバ31

(s)は、本明細書に記載の様々なタイプの装置12

(m)および13のいずれともすることができ、したがって、たとえば、パーソナル・コンピュータ、コンピュータ・ワークステーションおよび同様のものを含むことができ、これには、ネットワークに直接または間接に接続可能なそのような装置や他の多くのタイプの装置を含むミニ・コンピュータ、メインフレーム・コンピュータ、大容量記憶システム、計算サーバ、ローカル・エリア・ネットワーク(「LAN」)、およびワイド・エリア・ネットワーク(「WAN」)も含まれる。

【0018】前述のように、装置12(m)および装置13を含む装置は、インターネットを介してメッセージ・パケットを伝送することによって通信する。装置12(m)および13は、「ピアツーピア」方式、「クライアントーサーバ」方式、またはその両方の方式で情報を伝送することができる。一般に、「ピアツーピア」メッセージ・パケット伝送では、装置は1つまたは複数のメッセージ・パケットにした情報を他の装置に送信するに過ぎない。それに対して、「クライアントーサーバ」方式では、クライアントとして動作する装置が、サーバとして動作する他の装置にメッセージ・パケットを送信して、たとえば他方の装置によるサービスを開始することができる。たとえば他方の装置からの情報の検索、他方の装置が処理演算などを実行することができるようにすることなど、いくつかのタイプのこのようなサービスが、当業者にはわかるであろう。サーバがクライアントに情報を提供する場合、そのサーバは一般に記憶サーバと呼ぶことができる。それに対して、サーバがクライアントの要求により処理演算を実行する場合、そのサーバは一般に計算サーバと呼ぶことができる。クライアントの要求により他のタイプのサービスおよび操作を実行するサーバも、当業者ならわかるであろう。

【0019】クライアント/サーバ構成では、たとえば装置13によるサービスを必要とする装置12(m)は、必要なサービスを要求する1つまたは複数のメッセージ・パケットを生成して装置13に送信する。この要求メッセージ・パケットには、装置13、すなわち、メッセージ・パケットを受け取りサービスを実行する宛先装置のインターネット・アドレスが含まれる。装置12(m)は、要求メッセージ・パケットをISP11に送信する。ISP11は、そのメッセージ・パケットをインターネットを介して装置13に転送する。装置13がWANまたはLANの形態の場合、WANまたはLANがメッセージ・パケットを受け取り、それをそのWANまたはLANに接続され、要求されたサービスを提供する特定の装置に宛てて送る。

【0020】いずれの場合も、要求されたサービスを提供する装置13は、要求メッセージ・パケットを受け取った後、その要求を処理する。要求メッセージ・パケットを生成した装置12(m)またはその操作者が、装置

13に対して要求メッセージ・パケットを生成したそのサービスを要求するのに必要な許可を持っている場合、要求されたサービスが記憶サーバとしての装置13からクライアントとしての装置12(m)への情報の伝送を開始することである場合は、装置13は、要求された情報を含む1つまたは複数の応答メッセージ・パケットを生成し、そのパケットをインターネット14を介してISP11に送る。次にISP11はそのメッセージ・パケットを装置12(m)に送る。一方、要求されたサービスが計算サーバとしての装置13による処理を開始することである場合は、装置13は要求された計算サービスを実行する。さらに、装置13が計算中に生成された処理済みデータをクライアントとしての装置12(m)に返す必要がある場合、装置13は、処理済みデータを含む1つまたは複数の応答メッセージ・パケットを生成し、そのパケットをインターネット14を介してISP11に送る。次にISP11はそのメッセージ・パケットを装置12(m)に送る。サーバ装置13が提供できる他のタイプのサービスに関しても、対応する操作を装置12(m)および13、ISP11、およびインターネット14によって実行することができる。

【0021】上述のように、インターネット14を介して送信するために装置12(m)および13によって生成された各メッセージ・パケットには、スイッチング・ノードがそれぞれのメッセージ・パケットを適切な宛先装置に経路指定するために使用する宛先アドレスが含まれる。インターネットを介したアドレスは、「n」ビット整数の形態をとる(ただし「n」は現在、32または128とすることができる)。特に、装置12(m)の操作者が、インターネットを介した送信のためのメッセージ・パケットの生成を開始するために、特定のインターネット・アドレスを覚えてそれらを装置12(m)に供給しなくても済むようにするために、インターネットはそれぞれの装置の操作者がより容易に使用できる第2のアドレス指定機構を備える。このアドレス指定機構では、LAN、インターネット・サービス・プロバイダ(「ISP」)など、インターネットに接続されたインターネット・ドメインは、人間にとって比較的読みやすい名前でも識別される。人間可読ドメイン名に対応するために、ISP11は、ネームサーバ17(DNSサーバとも呼ばれることがある)に関連づけられている。ネームサーバは、人間可読ドメイン名を変換して、それぞれの人間可読名で呼ばれている宛先の適切なインターネット・アドレスを提供することができる。一般に、ネームサーバはISP11の一部とするか、または図1に示すようにISP11に直接接続することができる。あるいは、インターネットでISPを介してアクセス可能な特定の装置とすることもできる。いずれの場合も、前述のように、通信セッション中に装置12(m)がISP11にログオンすると、ISP11は、装置12(m)が

通信セッション中に使用する様々なインターネット・プロトコル(「IP」)パラメータを割り当てる。このパラメータはインターネット・パラメータ・ストア25に記憶される。これらのIPパラメータには、(a)通信セッション中に装置12(m)を識別するインターネット・アドレスと、(b)通信セッション中に装置12

(m)が使用するネームサーバ17の識別情報などの情報が含まれる。

【0022】装置12(m)は、送信のためにメッセージ・パケットを生成するとき、その装置12(m)のインターネット・アドレス(上記の項目(a))を送信元アドレスとして含める。それぞれのメッセージ・パケットを受け取る装置13は、装置12(m)から受け取ったメッセージ・パケットの中からこの送信元アドレスを使用することができ、それによって、それぞれの装置13によって生成されたメッセージ・パケットを装置12(m)に経路指定することができる。装置12(m)がインターネット14を介してネームサーバ17にアクセスする場合、ISP11によって提供されるネームサーバ識別情報(上記の項目(b))は、整数インターネット・アドレスの形態をとり、これによって、装置12(m)はネームサーバ17に対して人間可読インターネット・アドレスから整数インターネット・アドレスへの変換を要求するメッセージを生成することができる。ISP11は、装置12(m)がISP11にログオンすると、装置12(m)に他のIPパラメータも割り当てることができる。これには、たとえば、特にISPが複数のゲートウェイを有する場合に装置12(m)によって送信されるメッセージに使用されるインターネット14への接続の識別情報が含まれる。一般に、装置12(m)は、通信セッション中に使用するためにインターネット・パラメータをインターネット・パラメータ・ストア25に記憶する。

【0023】装置12(m)を操作する操作者が、装置12(m)から装置13にメッセージ・パケットを送信することができるようにしたい場合、操作者はオペレータ・インタフェース20を介して装置13のインターネット・アドレスと、そのメッセージで送信する装置12(m)が維持する情報またはその識別情報を装置12(m)に供給する。オペレータ・インタフェース20は、ISP11を介してインターネット14で送信するために、その必要なパケットに対してパケット・ジェネレータ22をイネーブルにする。パケット・ジェネレータ22は、(i)操作者が整数インターネット・アドレスを供給した場合、または(ii)操作者が人間可読インターネット・アドレスを供給したが、パケット・ジェネレータ22が操作者によって供給された人間可読インターネット・アドレスに対応するすでに整数インターネット・アドレスを持っている場合、オペレータ・インタフェース20によってイネーブルにされるとパケットを直

接生成し、それらをISP11に送信するためにネットワーク・インタフェース21に供給することができる。

【0024】しかし、操作者が、パケットの送信先である装置13の人間可読インターネット・アドレスを供給した場合、および、パケット・ジェネレータ22がまだそれに対応する整数インターネット・アドレスをもっていない場合、パケットジェネレータ22は、IPパラメータ・ストア25で識別されているネームサーバ17からネットワーク・アドレスを入手する。その操作に際して、パケット・ジェネレータ22は、最初にネームサーバ17に接触してネームサーバ17から適切な整数インターネット・アドレスの入手を試みる。これらの操作で、装置12(m)は、ネームサーバ17に送信するための適切なメッセージ・パケットを、装置12(m)が通信セッションの始めにログオンしたISP11によって提供されたネームサーバの整数インターネット・アドレスを使用して生成する。いずれの場合も、ネームサーバ17が人間可読名の整数インターネット・アドレスを持っているかまたは入手可能な場合、ネームサーバ17は装置12(m)に整数インターネット・アドレスを供給する。この整数インターネット・アドレスを、パケット・ジェネレータ22はネットワーク・インタフェース21およびパケット受信および処理機能要素23を介して受け取る。パケット・ジェネレータ22は整数インターネット・アドレスを受け取った後、ネットワーク・インタフェース21およびISP11を介して装置13に送信するために、必要なメッセージ・パケットを生成する。

【0025】前述のように、インターネット14に接続された装置13の1つは仮想私設ネットワーク15であり、この仮想私設ネットワーク15は、ファイアウォール30と、サーバ31(s)として識別された複数の装置と、ネームサーバ32とを含み、これらは通信リンク33によって相互接続されている。サーバ31(s)、ファイアウォール30、およびネームサーバ32は、LANまたはWANで接続された装置として、それらの装置の間でメッセージ・パケットの形態の情報を送信することができる。ファイアウォール30はインターネット14に接続され、インターネット14を介してメッセージ・パケットを受信することができるため、インターネット・アドレスを有する。さらに、少なくとも、インターネットを介してアクセスすることができるサーバ31(s)も、それぞれのインターネット・アドレスを有し、その接続で、ネームサーバ32は、仮想私設ネットワーク15内部のサーバ31(s)のための人間可読インターネット・アドレスをそれぞれの整数インターネット・アドレスに変換する役割を果たす。

【0026】一般に、仮想私設ネットワーク15は、サーバ31(s)が仮想私設ネットワーク15の外部の他の装置にアクセスしてその装置にインターネット14を

介して情報を送信することができるようにしたいが、装置12(m)およびその他の装置によるサーバ31

(s)へのインターネット14を介したアクセスを制御された方式で制限したい会社、政府機関、組織などによって維持されている。ファイアウォール30は、仮想私設ネットワーク15内のサーバ31(s)への、仮想私設ネットワーク15の外部の装置によるアクセスを制御する役割を果たす。その操作に際して、ファイアウォール30は、インターネット14にも接続し、インターネット14から、サーバ31(s)に送るためのメッセージ・パケットを受け取る。メッセージ・パケットが、メッセージ・パケットの送信元が特定のサーバ31(s)へのアクセスを要求していることを示している場合、および送信元がサーバ31(s)へのアクセスを許可されている場合、ファイアウォール30はメッセージ・パケットを通信リンク33を介してサーバ31(s)に転送する。他方、送信元がサーバ31(s)へのアクセスを許可されていない場合、ファイアウォール30はメッセージ・パケットをサーバ31に転送せず、その代わりに、送信元がサーバ31(s)へのアクセスを許可されていないことを示す応答メッセージ・パケットを送信元装置に送る。ファイアウォールは、仮想私設ネットワーク15内の他の装置31(s)と類似のものとすることができるが、参照番号43で一般的に示す、インターネットへの1つまたは複数の接続が追加されている。

【0027】装置12(m)などの仮想私設ネットワーク15の外部の装置と、仮想私設ネットワーク15内部のサーバ31(s)などの装置との間の通信は、前述のようにファイアウォール30と外部装置との間のセキュア・トンネルを介して維持することができ、それらの間で伝送される情報をインターネット14でISP11を介して伝送されている間機密に維持することができる。装置12(m)と仮想私設ネットワーク15との間のセキュア・トンネルは、図1で参照番号40、42、および44によって識別されている論理接続で表されている。論理接続42は、ISP11とインターネット14との間の論理接続41のうちの1つを含み、論理接続44はインターネット14とファイアウォール30の間の論理接続43のうちの1つを含むことがわかるであろう。

【0028】セキュア・トンネルの確立は、仮想ネットワーク15の外部である装置12(m)によって開始される。その操作に際して、装置12(m)は操作者からの要求に応答して、装置12(m)とファイアウォール30との間のセキュア・トンネルの確立を要求するメッセージ・パケットを生成し、ISP11およびインターネット14を介してファイアウォール30に送信する。メッセージ・パケットは、ファイアウォール30に関連づけられた所定の整数インターネット・アドレス宛てて送られる。そのアドレスは、セキュア・トンネル確立

要求のために取っており、ネームサーバ17にわかっており、ネームサーバ17によって装置12(m)に供給される。装置12(m)が仮想私設ネットワーク15内のサーバ31(s)へのアクセスを許可されている場合、クライアント12(m)とファイアウォール30は、インターネット14を介して両者の間で伝送される1つまたは複数のメッセージ・パケットを含む対話を行う。この対話中、ファイアウォール30は装置12

(m)に、仮想私設ネットワークが装置12(m)に送るメッセージ・パケットの暗号化された部分を装置12(m)が復号する際に使用する復号アルゴリズムとそれに付随する復号鍵の識別情報を提供することができる。さらに、ファイアウォール30は、装置12(m)に、装置12(m)が仮想私設ネットワーク15に送信するメッセージ・パケットの暗号化される部分を暗号化する際に装置12(m)が使用する、暗号化アルゴリズムとそれに付随する暗号鍵の識別情報も提供することができる。あるいは、装置12(m)がこの暗号化アルゴリズムと鍵の識別情報を提供することができ、それをファイアウォール30が対話中に使用する。装置12(m)は、ファイアウォール30の識別情報と、セキュア・トンネルを介して伝送されるメッセージ・パケットの暗号化アルゴリズムおよび復号アルゴリズムおよびそれらに付随する鍵の識別情報を関連づける情報を含む、セキュア・トンネルに関する装置12(m)のIPパラメータ25情報を記憶することができる。

【0029】その後、装置12(m)とファイアウォール30は、このセキュア・トンネルを介してメッセージ・パケットを送信することができる。装置12(m)は、セキュア・トンネルを介した転送のためにメッセージ・パケットを生成する際に、インターネット14を介してファイアウォール30に送信するためにネットワーク・インタフェース21によってISP11に送信する前に、メッセージ・パケットのうちの暗号化すべき部分を暗号化するためと、装置12(m)が受け取ったメッセージ・パケットの暗号化された部分を復号するために、セキュア・パケット処理機能要素26を使用する。具体的には、パケット・ジェネレータ22は、セキュア・トンネルを介してファイアウォール30に送信するためにメッセージ・パケットを生成した後、そのメッセージ・パケットをセキュア・パケット処理機能要素26に供給する。セキュア・パケット処理機能要素26は、暗号化アルゴリズムおよび鍵を使用して、メッセージ・パケットの暗号化すべき部分を暗号化する。ファイアウォール30は、セキュア・トンネルを介して装置12

(m)からメッセージ・パケットを受け取った後、それを復号し、メッセージ・パケットの意図された受信者が仮想私設ネットワーク15内のサーバ31(s)などの別の装置である場合、ファイアウォール30はメッセージ・パケットを通信リンク33を介してその別の装置に

送る。

【0030】セキュア・トンネルを介して仮想私設ネットワーク15内のサーバ31(s)などの装置によって装置12(m)に送信されるメッセージ・パケットの場合、ファイアウォール30はそのようなメッセージ・パケットを通信リンク33を介して受け取り、そのメッセージ・パケットを暗号化し、インターネット14を介してISP11に送る。ISP11はそのメッセージ・パケットを装置12(m)、詳細にはネットワーク・インタフェース21に転送する。ネットワーク・インタフェース21は、メッセージ・パケットをセキュア・パケット処理機能要素26に供給し、セキュア・パケット処理機能要素26は復号アルゴリズムおよび鍵を使用してメッセージ・パケットの暗号化部分を復号する。

【0031】仮想私設ネットワーク15の外部にある装置12(m)などの装置と、ファイアウォールの外部にあるサーバ31(s)などの装置によるアクセスに関して問題が生じる。すなわち、ネームサーバ17に、ファイアウォール30に関連づけられた整数インターネット・アドレス以外の、仮想私設ネットワーク15内にあるサーバ31(s)およびその他の装置の整数インターネット・アドレスが提供されてないことである。したがって、装置12(m)は、操作者が人間可読インターネット・アドレスを入力した後で、そのネームサーバ17からアクセスされるサーバ31(s)の整数インターネット・アドレスを入手することができない。

【0032】この問題に対処するために、装置12

(m)とファイアウォール30が協調して両者の間にセキュア・トンネルを確立するときに、セキュア・トンネルを介して送信されるメッセージ・パケットと共に使用される暗号化および復号のアルゴリズムおよび鍵の識別情報を装置12(m)に提供することができる他に、ファイアウォール30は装置12(m)に対して、装置12(m)の操作者が供給することができる人間可読インターネット・アドレスの適切な整数インターネット・アドレスを装置12(m)が入手するためにアクセスできる、仮想私設ネットワーク15内のネームサーバ32などのネームサーバの識別情報も提供する。ネームサーバ32の識別情報も、通信セッションの始めに装置12(m)がISP11にログオンしたときにISP11によって提供されたネームサーバ17の識別情報と共にIPパラメータ・ストア25に記憶される。したがって、装置12(m)が、たとえば操作者によって供給された人間可読インターネット・アドレスを使用して、仮想私設ネットワーク15内のサーバ31(s)などの装置にメッセージ・パケットを送信する場合、装置12(m)は前述のように最初にネームサーバ17にアクセスして、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスの入手を試行する。ネームサーバ17は仮想私設ネットワーク15の外部にあ

り、装置12(m)によって要求された情報を持たないため、それを示す応答メッセージ・パケットを送信する。装置12(m)はその後で、要求メッセージ・パケットを生成し、ファイアウォール30とセキュア・トンネルを介してネームサーバ32に送信する。ネームサーバ32が装置12(m)によって供給された要求メッセージ・パケット内の人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っている場合、ネームサーバ32はネームサーバ17に関連して前述したのとほぼ同様の方式で整数インターネット・アドレスを提供する。ただし、ネームサーバ32は、この整数インターネット・アドレスをファイアウォール30に宛てられたメッセージ・パケットで供給し、ファイアウォール30はその後でそのメッセージ・パケットをセキュア・トンネルを介して装置12(m)に送信する。ファイアウォール30によって送信されるメッセージ・パケットでは、メッセージ・パケット内の整数インターネット・アドレスはセキュア・トンネルを介して伝送されるメッセージ・パケットのデータ部分に入れられ、したがって、暗号化形式をとる。メッセージ・パケットは、装置12(m)がセキュア・トンネルを介して受け取る他のメッセージ・パケットに関して前述したと同様の方式で装置12(m)によって処理される。すなわち、メッセージ・パケットは、処理のためにパケット受信および処理機能要素23に供給される前に、セキュア・パケット処理機能要素26によって復号される。サーバ31(s)の整数インターネット・アドレスは、それに対する人間可読インターネット・アドレスとの関連づけと、その人間可読インターネット・アドレスに関連づけられたサーバ31(s)に仮想私設ネットワーク15のファイアウォールを介してアクセスする必要があることを示す標識と、サーバ31(s)に対して送信され、サーバ31(s)が受け取るメッセージ・パケットの適切な部分の暗号化および復号に使用される暗号化および復号のアルゴリズムおよび鍵の識別情報と共に、IPパラメータ・ストア25内のアクセス制御リスト(「ACL」)にキャッシュすることができる。

【0033】装置12(m)によって供給された人間可読インターネット・アドレスの整数インターネット・アドレスをネームサーバ32に要求する装置12(m)からのメッセージ・パケットにネームサーバが応答する際、ネームサーバ32がその人間可読インターネット・アドレスと整数インターネット・アドレスとの間の関連づけを持っていない場合、ネームサーバ32はそれを示す応答メッセージ・パケットを送ることができる。装置12(m)が、装置12(m)がアクセスすることができる他の仮想私設ネットワーク(図示せず)に関連づけられている可能性のあるネームサーバなど、他のネームサーバの識別情報を持っている場合、装置12(m)は上述と同様の方式で他のネームサーバにアクセスを試み

ることができる。装置12(m)が、アクセスすることができ、装置12(m)のIPパラメータ・ストア25内で一般的に識別されるいずれのネームサーバからもその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを入手することができない場合、装置12(m)は、人間可読インターネット・アドレスを持っている装置にアクセスすることができず、アクセスを要求した操作者またはプログラムにそれを通知する。

【0034】これを背景にして、本発明と共に装置12(m)および仮想私設ネットワーク15によって実行される操作について以下に詳述する。一般に、操作は2段階で進む。第1段階では、装置12(m)と仮想私設ネットワーク15が協調して、インターネット14を介したセキュア・トンネルを確立する。この第1段階で、仮想私設ネットワーク15、詳細にはファイアウォール30が、ネームサーバ32の識別情報を提供し、前述のように暗号化および復号のアルゴリズムおよび鍵情報も提供することができる。第2段階では、セキュア・トンネルが確立された後、装置12(m)は、第1段階中にファイアウォール30によって識別されたネームサーバ32から、必要に応じて人間可読インターネット・アドレスから整数インターネット・アドレスへの変換を入手するプロセスで、仮想私設ネットワーク15内の1つまたは複数のサーバ31(s)へのメッセージ・パケットの生成と送信に関して第1段階で提供された情報を使用することができる。

【0035】したがって、第1の(セキュア・トンネル確立)段階では、装置12(m)は最初に、ファイアウォール30への送信のためにセキュア・トンネルの確立を要求するメッセージ・パケットを生成する。このメッセージ・パケットには、ファイアウォールの整数インターネット・アドレス(装置の操作者または装置12(m)によって処理されているプログラムによって供給されたか、または操作者またはプログラムによって人間可読インターネット・アドレスが供給された後でネームサーバ17によって供給されたもの)、詳細には、ファイアウォール30がそれとのセキュア・トンネルを確立することができるようにするためのアドレスが含まれる。ファイアウォール30がセキュア・トンネル確立要求を受け入れる場合、およびファイアウォール30が前述のように暗号化および復号アルゴリズムおよび鍵を提供する場合、ファイアウォールは、その暗号化および復号アルゴリズムおよび鍵を識別する応答メッセージ・パケットを、装置12(m)への送信のために生成する。装置12(m)が応答メッセージを受け取ると、暗号および復号アルゴリズムおよび復号アルゴリズムおよび鍵の識別情報はIPパラメータ・ストア25に記憶される。

【0036】第1段階のうちの後の時点で、ファイアウ

オール30は、装置12(m)に送信するためにネームサーバ32の整数インターネット・アドレスを含むメッセージ・パケットも生成する。このメッセージ・パケットの場合、メッセージ・パケットのうちのネームサーバ32の整数インターネット・アドレスを含む部分が、暗号化アルゴリズムおよび鍵を使用して暗号化され、それを、前述の応答メッセージ・パケットで提供される復号アルゴリズムおよび鍵を使用して復号することができる。このメッセージは一般に以下のような構造を有する。

"<IIA(FW), IIA(DEV12(m))>SEC_TUN><ENCR<<IIA(FW), IIA(DEV12(m))><DNS_ADRS:IIA(NS32)>>>" 上記で、(i)"IIA(FW)"は送信元アドレス、すなわちファイアウォール30の整数インターネット・アドレスを表し、(ii)"IIA(DEV12(m))"は宛先アドレス、すなわち装置12(m)の整数インターネット・アドレスを表し、(iii)"DNS_ADRS:IIA(NS)"は、"IIA(NS32)"が装置12(m)が使用を許可されているネームサーバ32の整数インターネット・アドレスを表すことを示し、(iv)"ENCR<...>"は、大括弧"<"と">"の間の情報が暗号化されることを示す。メッセージの最初の部分最初の部分"<IIA(FW), IIA(DEV12(m))>"は、メッセージのヘッダ部の少なくとも一部を形成し、"<ENCR<<IIA(FW), IIA(DEV12(m))><IIA(NS)>>>"は、メッセージのデータ部の少なくとも一部を表す。"<SEC_TUN>"は、ヘッダ内のセキュア・トンネルを介して伝送されるメッセージを示す標識を表し、それによってメッセージのデータ部に暗号化情報が含まれていることを示す。

【0037】装置12(m)が前述のようにファイアウォール30からメッセージを受け取った後、メッセージ・パケットには<SEC_TUN>標識が含まれているため、装置12(m)のネットワーク・インタフェース21は暗号化部分"<ENCR<<IIA(FW), IIA(DEV12(m))><DNS_ADRS:IIA(NS32)>>>"を、処理のためにセキュア・パケット処理機能要素26に送る。セキュア・パケット処理機能要素は、暗号化部分を復号し、"IIA(NS32)"部分がネームサーバ、装置12(m)が使用することを許可されている特にネームサーバ32の整数インターネット・アドレスであると判断し、そのアドレスを、それに送られるメッセージ・パケットがファイアウォール30に転送すべきであることと、ファイアウォール30によって前もって提供された暗号化アルゴリズムおよび鍵を使用してメッセージ・パケット内のデータを暗号化すべきであることを示す標識と共に、I

Pパラメータ・ストア25に記憶する。ネームサーバ32の整数インターネット・アドレスはファイアウォールから装置12(m)に暗号化形式で送られるため、パケットが第三者によって傍受された場合でも機密に維持される。

【0038】セキュア・トンネルの確立に使用される特定のプロトコルによっては、ファイアウォール30と装置12(m)は上述の情報以外の情報を含むメッセージ・パケットを交換することもできる。

【0039】前述のように、第2段階では、セキュア・トンネルが確立された後、装置12(m)は第1段階中に提供された情報を、メッセージ・パケットの生成と、仮想私設ネットワーク15内のサーバ31(s)のうちの1つまたは複数のサーバへの送信に関して使用することができる。これらの操作に際して、装置12(m)の操作者または装置12(m)によって処理されているプログラムが、装置12(m)に仮想私設ネットワーク15内のサーバ31(s)に対してメッセージ・パケットを送信させたい場合、オペレータ・インタフェース20を介して操作者が、またはプログラムが人間可読インターネット・アドレスを供給した場合、装置12(m)、詳細にはパケット・ジェネレータ22は、最初にIPパラメータ・ストア25がその中にその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスをキャッシュしているかどうかを判断する。キャッシュしていない場合、パケット・ジェネレータ22は、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを供給するように要求する要求メッセージ・パケットを生成し、ネームサーバ17に送る。ネームサーバがその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っている場合、ネームサーバ17はその整数インターネット・アドレスを装置12(m)に供給する。これは、要求メッセージ・パケット内の人間可読インターネット・アドレスが仮想私設ネットワーク15の外部の装置13に関連づけられていた場合にも、仮想私設ネットワーク15内のサーバ32(s)に関連づけられていた場合にも行われれることがわかるであろう。その後、装置12(m)は、前述のように、インターネットを介して送信するためにその整数インターネット・アドレスを使用してメッセージ・パケットを生成することができる。

【0040】一方、ネームサーバ17がその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っていない場合、ネームサーバ17は装置12(m)にそれを示す応答メッセージ・パケットを送る。その後、装置12(m)のパケット・ジェネレータ22が、そのIPパラメータ・ストア25で識別されている次のネームサーバに送信するための要求メッセージ・パケットを生成し、そのネームサーバに対し

てその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを提供するように要求する。この、次のネームサーバがネームサーバ32である場合、パケット・ジェネレータ22はメッセージ・パケットを処理のためにセキュア・パケット処理機能要素26に送る。セキュア・パケット処理機能要素26は、セキュア・トンネルを介してファイアウォール30に送る要求メッセージ・パケットを生成する。このメッセージは一般に以下のような構造を有する。

" < I I A (DEV_12 (m)) , I I A (FW) > < SEC_TUN > < ENCR < < I I A (DEV_12 (m)) , I I A (NS_32) > > < I I A_REQ > > " 上記で、(i) " < I I A (DEV_12 (m)) " は送信元アドレス、すなわち装置12 (m) の整数インターネット・アドレスを表し、(ii) " I I A (FW) " は宛先アドレス、すなわちファイアウォール30の整数インターネット・アドレスを表し、(iii) " I I A (NS_32) " はネームサーバ32のアドレスを表し、(iv) " < I I A (DEV_12 (m)) , I I A (NS_32) > > < I I A_REQ > > " は、パケット・ジェネレータ22によって生成された要求メッセージ・パケットを表し、" < I I A (DEV_12 (m)) , I I A (NS_32) > " は要求メッセージ・パケットのヘッダ部を表し、" < I I A_REQ > " は要求メッセージ・パケットのデータ部を表し、(v) " ENCR < . . . > " は、大括弧" < " と" > " の間の情報が暗号化されていることを表し、(vi) " < SEC_TUN > " は、セキュア・パケット・ジェネレータ22によって生成されたメッセージ・パケットのヘッダ部内にある標識であって、メッセージがセキュア・トンネルを介して送信されることを示し、それによって、メッセージのデータ部に暗号化情報が含まれていることを示す。

【0041】ファイアウォール30は、セキュア・パケット処理機能要素26によって生成された要求メッセージ・パケットを受け取ると、メッセージ・パケットの暗号化部分を復号して、要求メッセージ・パケットがパケット・ジェネレータ22によって生成されたことを表す" < I I A (DEV_12 (m)) , I I A (NS_32) > > < I I A_REQ > > " を入手する。要求メッセージ・パケットを入手した後、ファイアウォール30はそれを通信リンク33を介してネームサーバ32に送る。このプロセスの際、通信リンク33を介してメッセージ・パケットを送信するプロトコルによっては、ファイアウォール30は通信リンク33のプロトコルに準拠するように要求パケットを修正する必要がある場合もある。

【0042】ネームサーバ32は、要求メッセージ・パケットを受け取った後、それを処理して、ネームサーバ32が要求メッセージ・パケットで供給された人間可読

インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っているかどうかを判断する。ネームサーバがそのような整数インターネット・アドレスを持っていると判断した場合、ネームサーバはファイアウォールに送信するためにその整数インターネット・アドレスを含む応答メッセージ・パケットを生成する。一般に、この応答メッセージ・パケットは以下の構造を有する。

< < I I A (NS_32) , I I A (DEV_12 (m)) > < I I A_RESP > > 上記で、(i) " I I A (NS_32) " は送信元アドレス、すなわちネームサーバ32の整数インターネット・アドレスを表し、(ii) " I I A (DEV_12 (m)) " は宛先アドレス、すなわち装置12 (m) の整数インターネット・アドレスを表し、(iii) " I I A_RESP " は、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを表す。

【0043】ファイアウォール30が応答メッセージ・パケットを受け取った後、装置12 (m) との通信が両者の間のセキュア・トンネルを介するため、ファイアウォール30はネームサーバ32から受け取った応答メッセージ・パケットを暗号化し、装置12 (m) に送信するためにその暗号化応答メッセージ・パケットを含むメッセージ・パケットを生成する。一般に、ファイアウォール30によって生成されるメッセージ・パケットは以下の構造を有する。" < I I A (FW) , I I A (DEV_12 (m)) > < SEC_TUN > < ENCR < < I I A (NS_32) , I I A (DEV_12 (m)) > > < I I A_RESP > > " 上記で、(i) " I I A (FW) " は送信元アドレス、すなわちファイアウォール30の整数インターネット・アドレスを表し、(ii) " I I A (DEV_12 (m)) " は宛先アドレス、すなわち装置12 (m) の整数インターネット・アドレスを表し、(iii) " SEC_TUN " は、セキュア・パケット・ジェネレータ22によって生成されたメッセージ・パケットのヘッダ部内の、メッセージがセキュア・トンネルを介して送信されることを示す標識を表し、それによってメッセージのデータ部に暗号化情報が含まれていることを示し、(iv) " ENCR < . . . > " は、" < " と" > " の間の情報 (ネームサーバ32から受け取った応答メッセージ・パケットを構成する) が暗号化されていることを示す。

【0044】さらに、通信リンク33を介したメッセージ・パケットの送信のためのプロトコルによっては、ファイアウォール30はインターネット14のプロトコルに準拠するようにメッセージ・パケットを処理および/または修正する必要がある場合がある。

【0045】装置12 (m) がファイアウォール30からメッセージ・パケットを受け取ると、そのメッセージ・パケットはセキュア・パケット処理機能要素26に送

られる。セキュア・パケット処理機能要素26は、メッセージ・パケットの暗号化部分を復号し、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを入手し、その情報をIPパラメータ・ストア25にロードする。その後、装置はその整数インターネット・アドレスを、人間可読インターネット・アドレスに関連づけられたサーバ31(s)に送信するためのメッセージ・パケットの生成に使用することができる。

【0046】要求メッセージ・パケットで装置12

(m) から送られた人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスをネームサーバ32が持っていなかった場合、ネームサーバ32はネームサーバ32によって生成される応答メッセージ・パケットでそれを示すことができることがわかるであろう。ファイアウォール30は、ネームサーバ32から送られた応答メッセージに回答し、装置12(m)に送信するために、ネームサーバ32によって生成された応答メッセージ・パケットを含む暗号化部分が入ったメッセージ・パケットも生成する。装置12(m)がメッセージ・パケットを受け取った後、暗号化部分はセキュア・パケット処理機能要素26によって復号され、セキュア・パケット処理機能要素26はパケット・ジェネレータ22に、その人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスをネームサーバ32が持っていないことを通知する。その後、IPパラメータ・ストア25に別のネームサーバの識別情報が入っている場合、装置12(m)のパケット・ジェネレータ22はそのIPパラメータ・ストア25で識別されている次のネームサーバに送信するために要求メッセージ・パケットを生成し、そのネームサーバに人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを供給するように要求する。それに対して、IPパラメータ・ストア25に別のネームサーバの識別情報が入っていない場合、パケット・ジェネレータ22は、オペレータ・インタフェース20またはプログラムに対して、それによって供給された人間可読インターネット・アドレスに関連づけられた装置に送信するためのメッセージ・パケットを生成することができないことを通知する。

【0047】本発明にはいくつかの利点がある。具体的には、本発明は、セキュア・トンネルを介して私設ネットワークに接続されたネームサーバによる人間可読アドレスからネットワーク・アドレスへの変換を容易にすることによって、インターネット14などの公衆ネットワークに接続された装置と、仮想私設ネットワーク15などの私設ネットワークに接続された装置と間の通信を容易にするシステムを提供する。

【0048】図1に関して前述した構成には多くの変更を加えることができることがわかるであろう。たとえ

ば、ネットワーク10について、暗号化および復号のアルゴリズムおよび鍵が、セキュア・トンネルが確立される対話中に装置12(m)とファイアウォールとの間で交換されるものとして説明したが、この情報は装置12(m)とファイアウォール30によって両者の間のセキュア・トンネルの確立とは別に提供することもできることがわかるであろう。

【0049】さらに、本発明についてインターネットに関して説明したが、本発明はどのようなネットワークと共にでも利用可能であることがわかるであろう。さらに、本発明について、人間可読ネットワーク・アドレスを備えるネットワークに関して説明したが、本発明はどのような形態の二次または非公式ネットワーク・アドレス構成を備えるどのようなネットワークと共にでも利用可能であることがわかるであろう。

【0050】本発明によるシステムは全部または一部を、特殊目的のハードウェアまたは汎用コンピュータ・システム、あるいはその任意の組合せで構成することができ、そのどの部分も適合するプログラムによって制御可能であることがわかるであろう。どのプログラムもその全部または一部が、従来の方式でシステムの一部を含むかまたはシステム上に記憶することができる。あるいは、プログラムの全部または一部を従来の方式で情報を伝送するネットワークまたはその他の機構を介してシステム内に供給することができる。さらに、このシステムは、システムに直接接続可能な、または従来の方式で情報を伝送するネットワークまたはその他の機構を介してシステムに情報を伝送することができる操作者入力要素(図示せず)を使用して、操作者によって供給される情報を使用して操作および/または制御することができることがわかるであろう。

【0051】以上の説明は、本発明の特定の実施形態に限られていた。しかし、本発明には様々な変形または修正を加えることができ、その際、本発明の利点の一部または全部が実現されることがわかるであろう。特許請求の範囲の目的は、上記およびその他の変形および修正を、本発明の精神および範囲に含まれるものとしてカバーすることである。

【図面の簡単な説明】

【図1】 本発明により構成されたネットワークを示す機能ブロック図である。

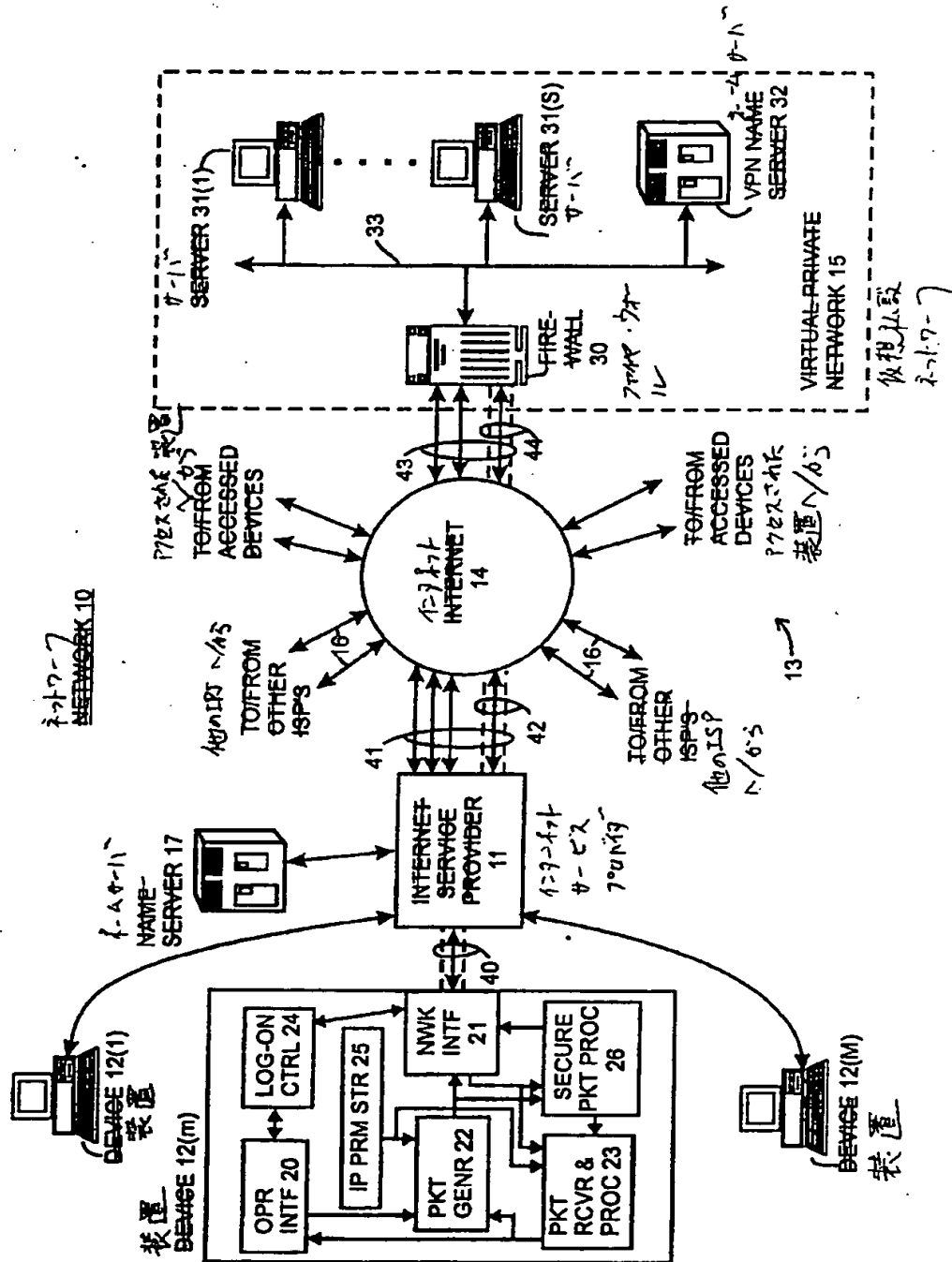
【符号の説明】

- 10 ネットワーク
- 12、13 装置
- 15 仮想私設ネットワーク
- 17 ネームサーバ
- 20 オペレータ・インタフェース
- 21 ネットワーク・インタフェース
- 22 パケット・ジェネレータ
- 23 パケット受信および処理機能要素

- 24 ログオン・コントロール
 25 インターネット・パラメータ・ストア
 26 セキュア・パケット処理機能要素

- 30 ファイアウォール
 31 サーバ
 32 ネームサーバ

【図1】



フロントページの続き

(71)出願人 591064003

901 SAN ANTONIO ROAD
PALO ALTO, CA 94303, U.
S. A.

(72)発明者 ジョセフ・イー・プロビーノ

アメリカ合衆国・02138・マサチューセッ
ツ州・ケンブリッジ・ウェンデル ストリ
ート・29

THIS PAGE BLANK (USPTO)